Configura VPN basata su route con route statica su FTD Gestito da FDM

Sommario

[Introduzione](#)

[Prerequisiti](#)

- [Requisiti](#)
- [Componenti usati](#)
- [Premesse](#)

[Procedura di configurazione in FDM](#)

[Verifica](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come configurare un sito basato su route statica per il tunnel VPN del sito su un FTD gestito da FDM.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza base del funzionamento di un tunnel VPN.
- Conoscenza preliminare della navigazione in Firepower Device Manager (FDM).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

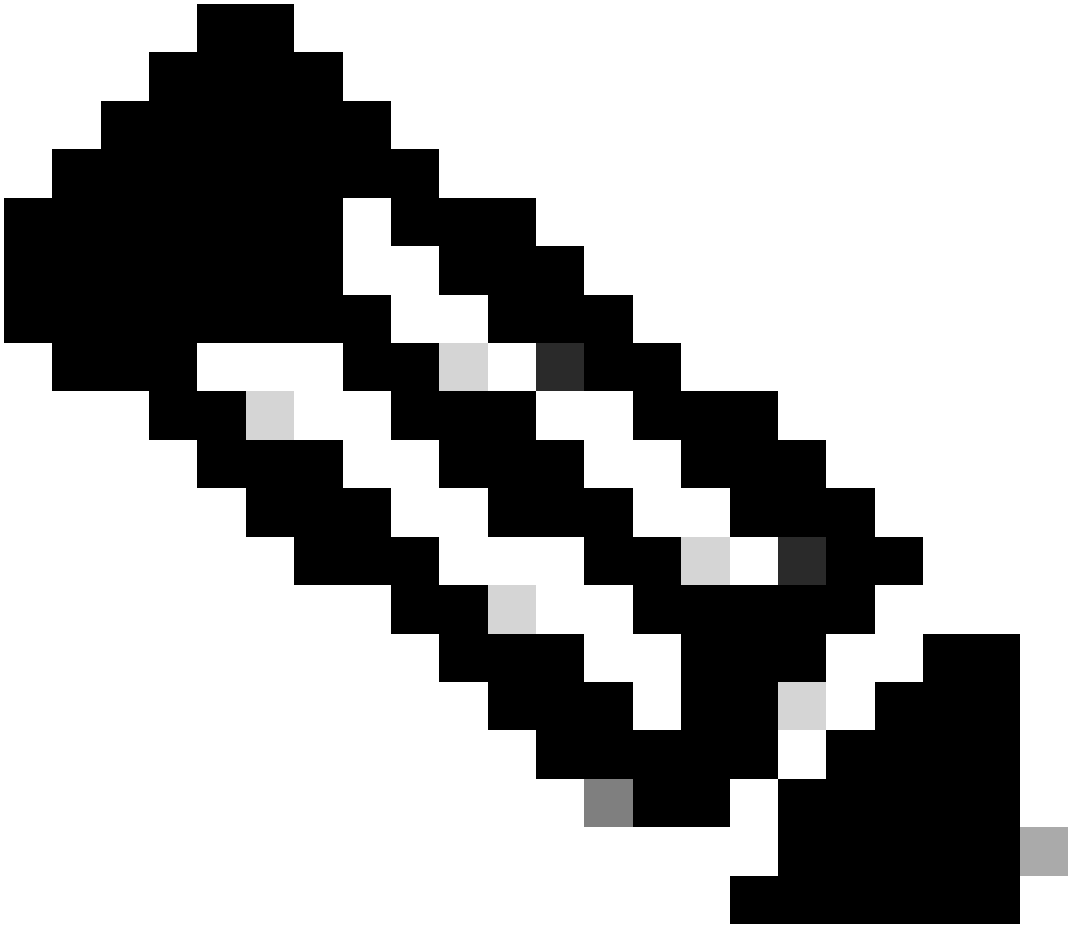
- Cisco Firepower Threat Defense (FTD) versione 7.0 gestito da Firepower Device Manager (FDM).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La VPN basata su route consente di determinare il traffico interessante da crittografare o inviare tramite il tunnel VPN e di utilizzare il routing del traffico anziché criteri/elenchi di accesso come nella VPN basata su criteri o su mappa crittografica. Il dominio di crittografia è impostato per consentire il traffico in entrata nel tunnel IPsec. I selettori di traffico locale e remoto di IPSec sono impostati su 0.0.0.0/0.0.0.0. Ciò significa che tutto il traffico instradato nel tunnel IPSec viene crittografato indipendentemente dalla subnet di origine/destinazione.

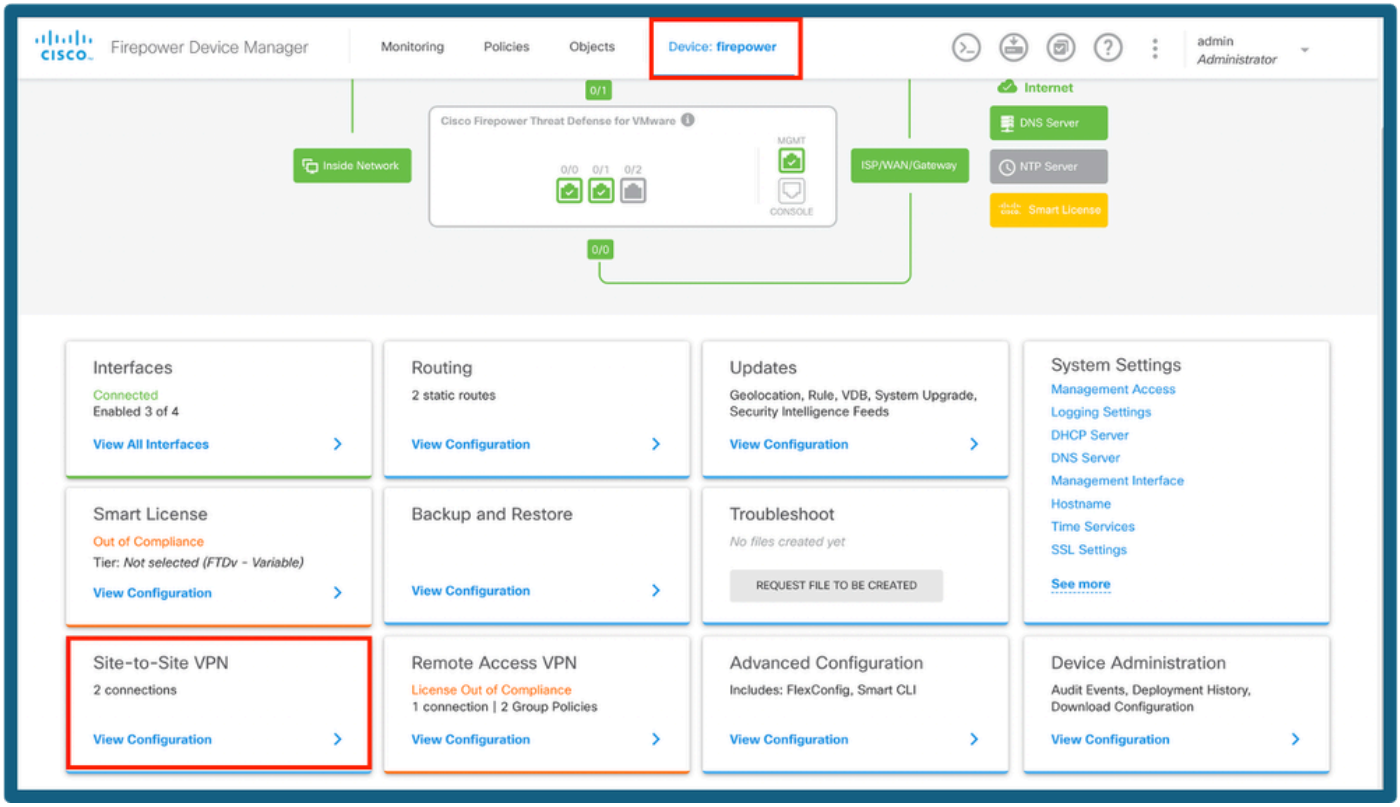
Nel documento si fa riferimento alla configurazione SVTI (Static Virtual Tunnel Interface).



> Nota: Non sono necessarie licenze aggiuntive. La VPN basata su route può essere configurata sia in modalità di licenza che in modalità di valutazione. Senza la conformità alla crittografia (funzionalità di esportazione controllate abilitate), solo DES può essere utilizzato come algoritmo di crittografia.

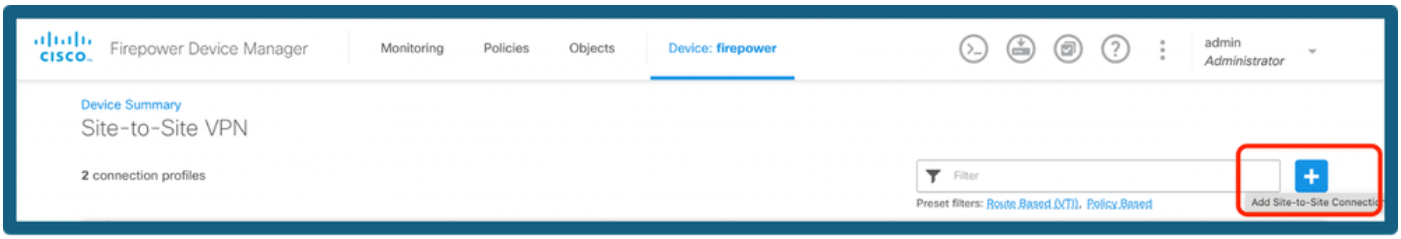
Procedura di configurazione in FDM

Passaggio 1. Passare a Dispositivo > Da sito a sito.



Dashboard FDM

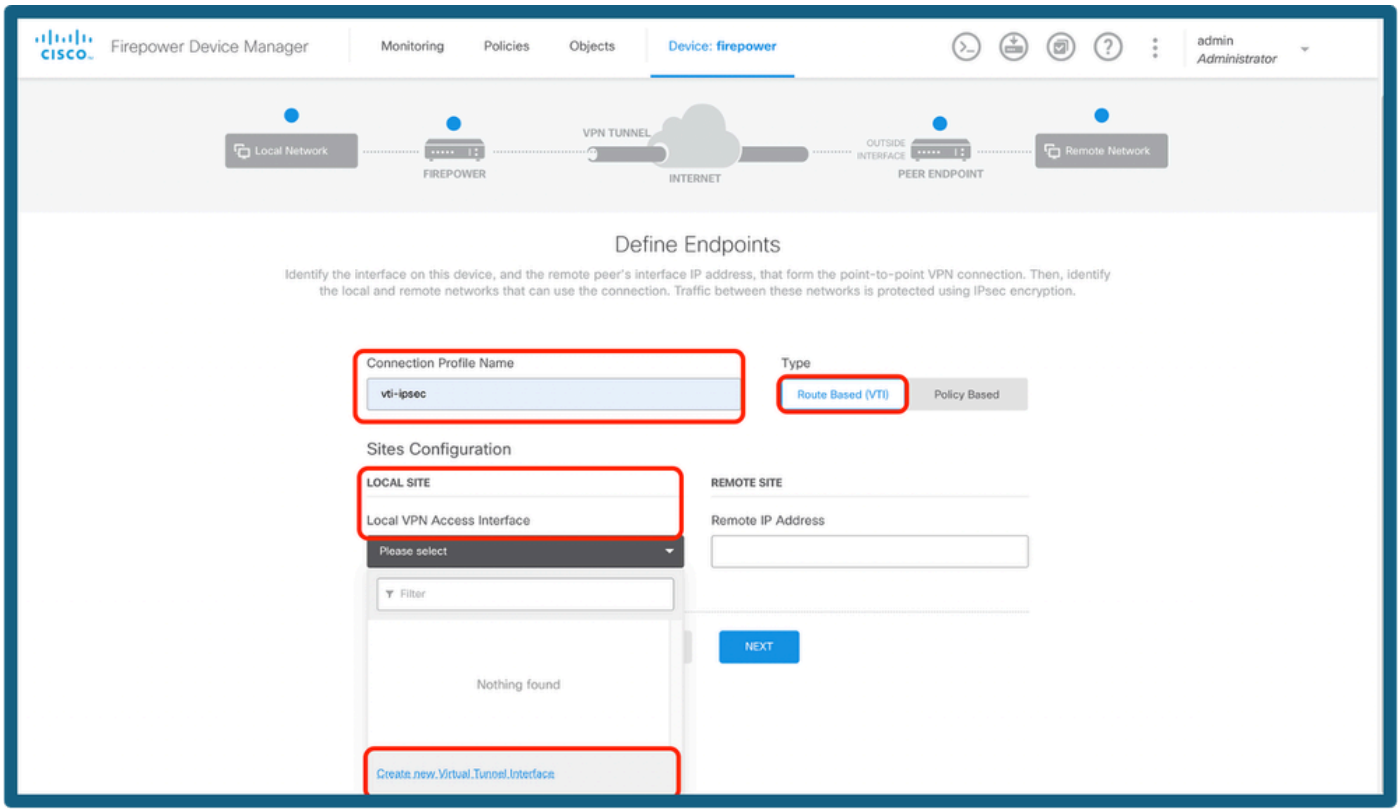
Passaggio 2. Fare clic sull'icona + per aggiungere un nuovo sito alla connessione.



Aggiungi connessione da sito a sito

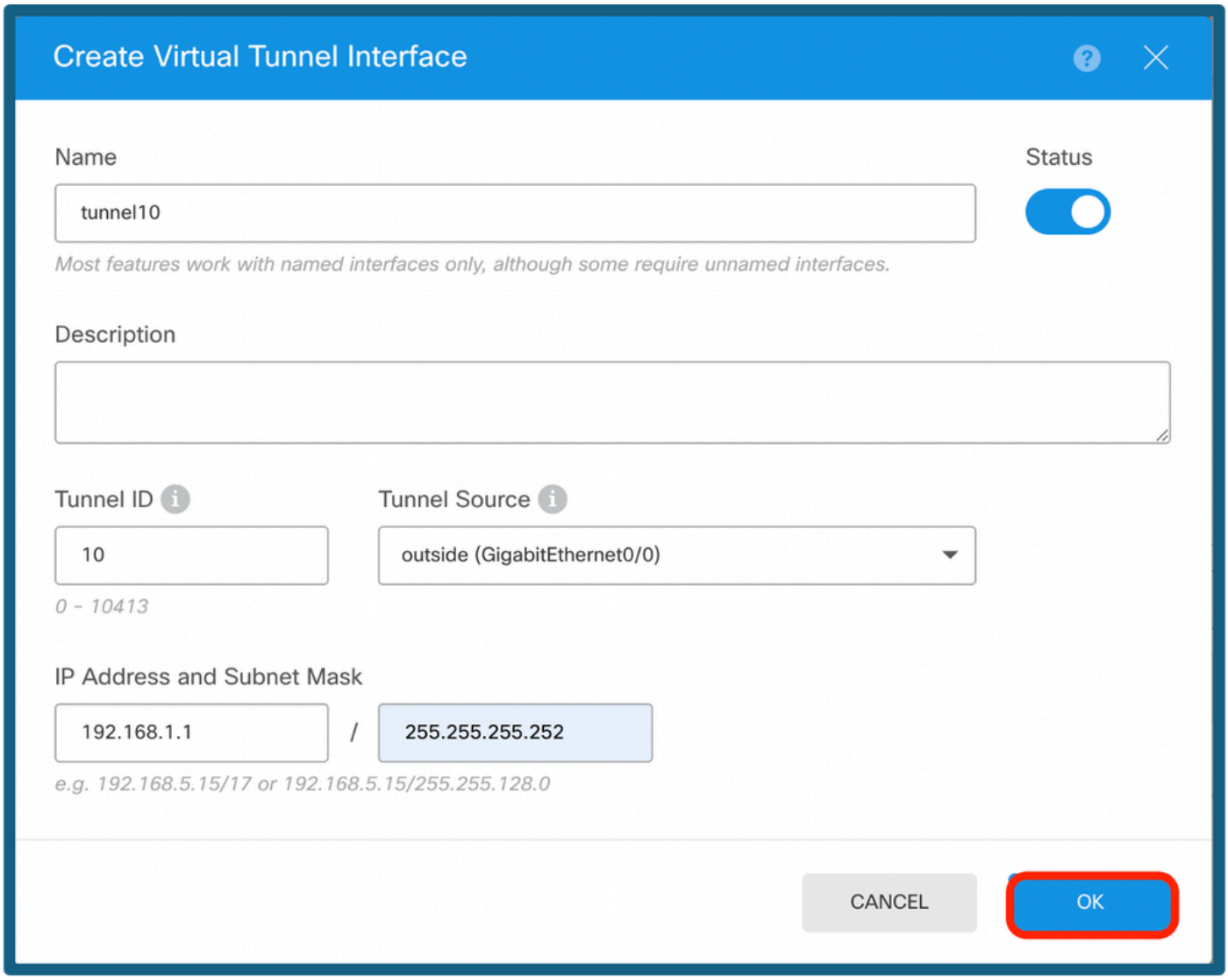
Passaggio 3. Fornire un nome di topologia e selezionare il tipo di VPN come VTI (Route Based).

Fare clic su Local VPN Access Interface (Interfaccia di accesso VPN locale) e quindi su Create new Virtual Tunnel Interface (Crea nuova interfaccia tunnel virtuale) o selezionarne una dall'elenco esistente.



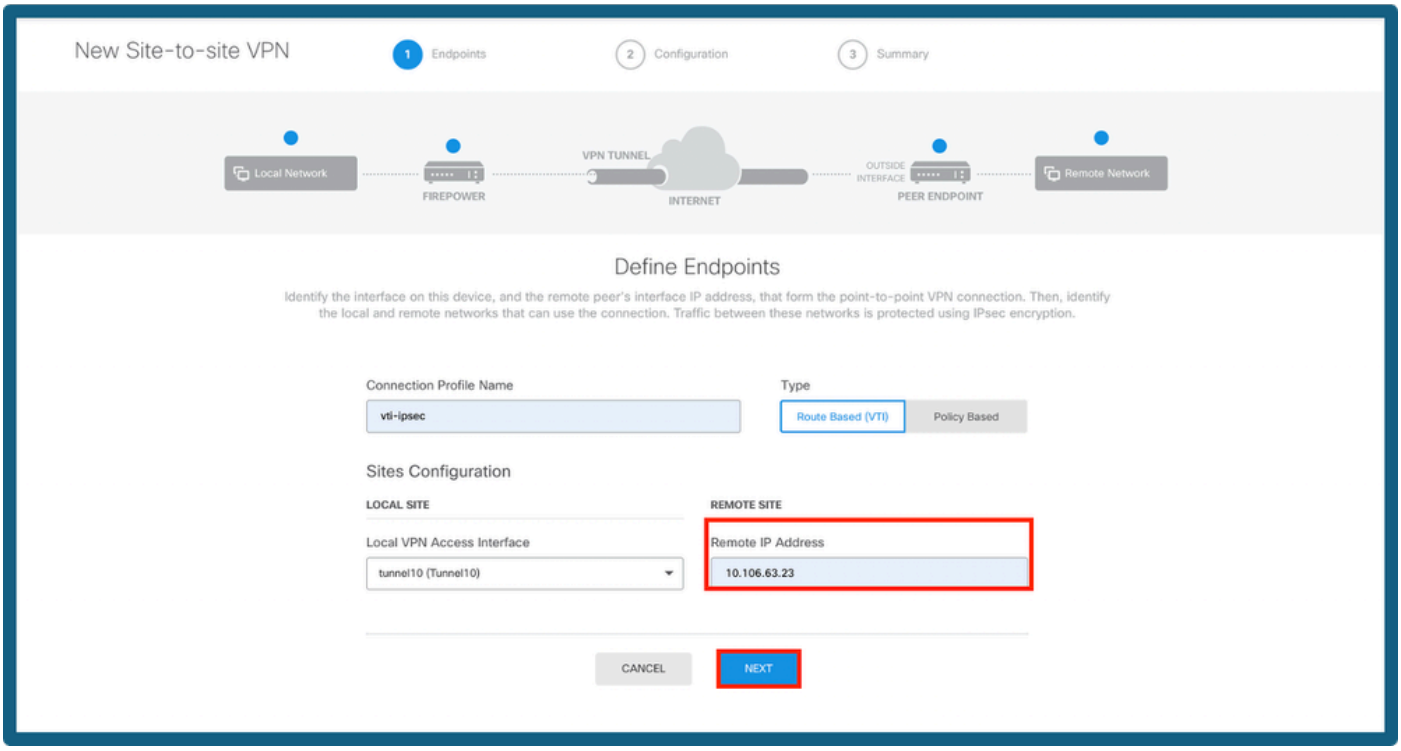
Aggiungi interfaccia tunnel

Passaggio 4. Definire i parametri della nuova interfaccia del tunnel virtuale. Fare clic su OK.



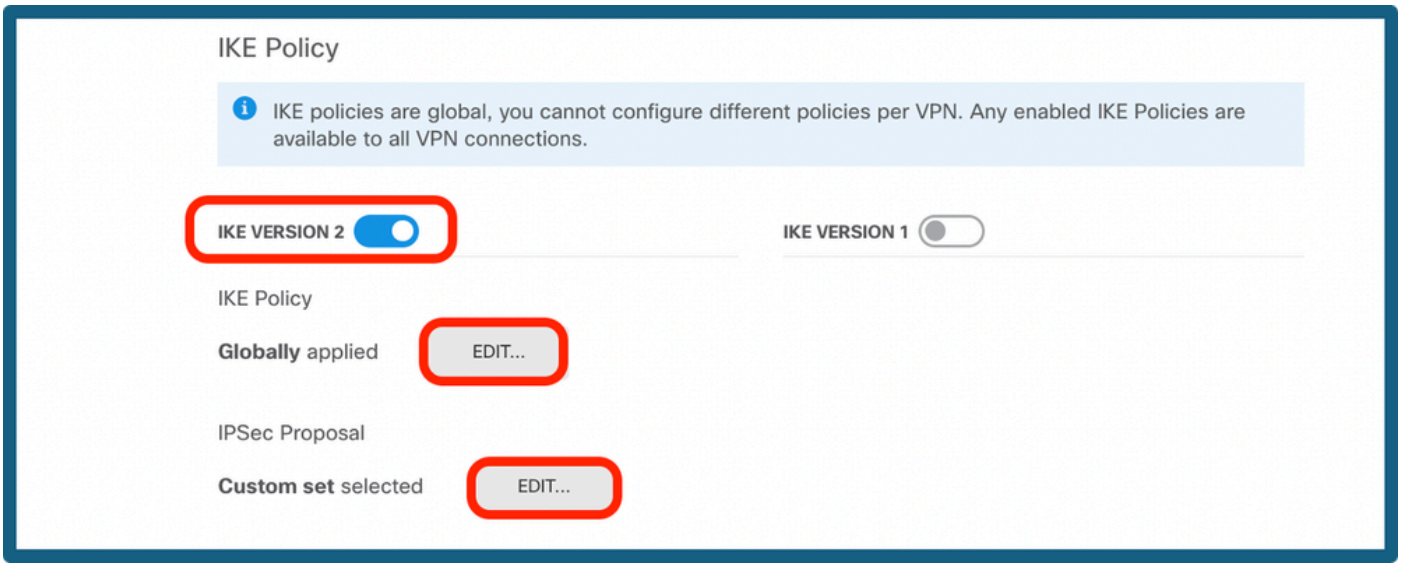
Configurazione VTI

Passaggio 5. Scegliere la VTI appena creata o una VTI esistente in Virtual Tunnel Interface. Fornire l'indirizzo IP remoto.



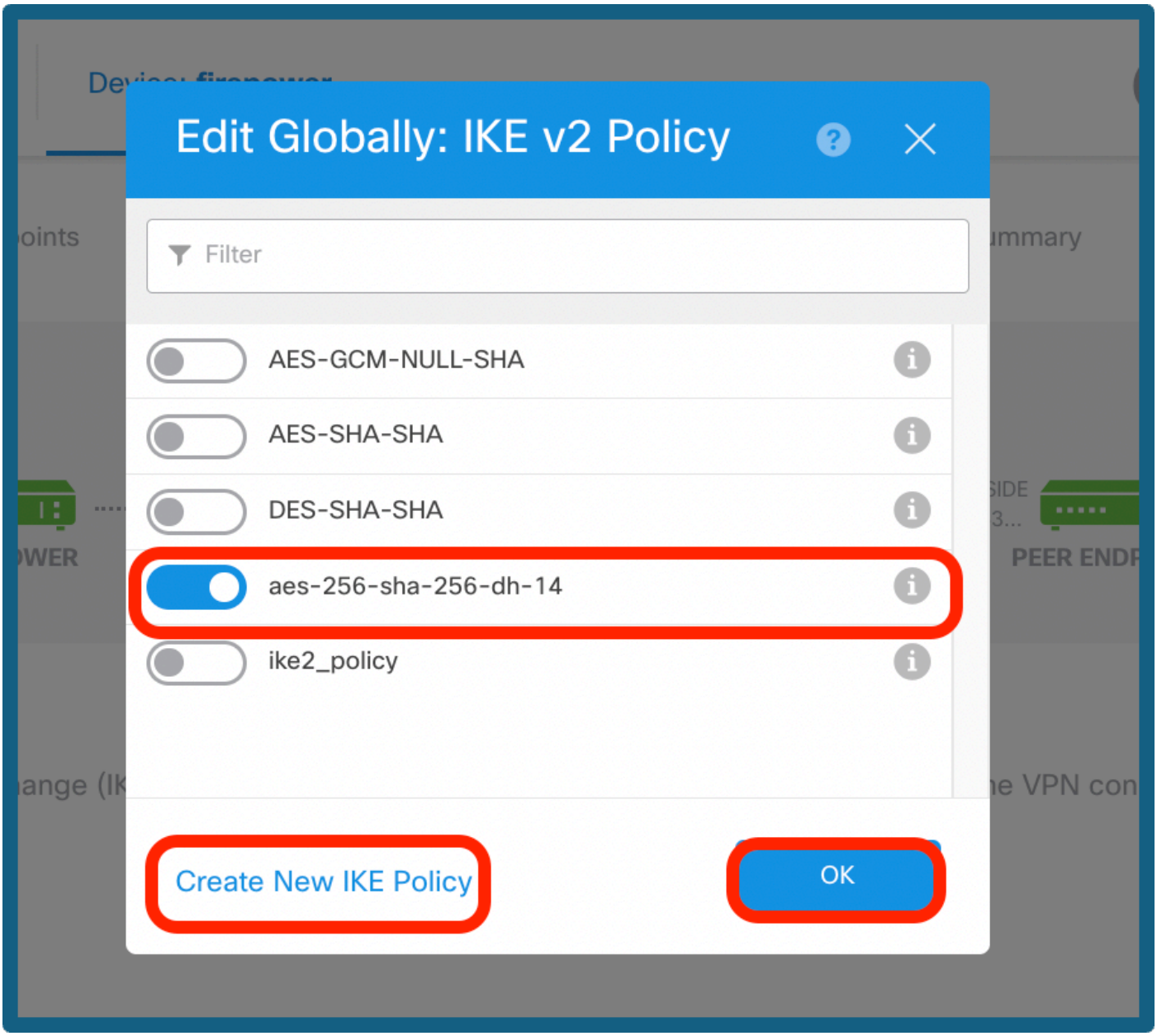
Aggiungi IP peer

Passaggio 6. Scegliere IKE Version, quindi il pulsante Edit (Modifica) per impostare i parametri IKE e IPsec come mostrato nell'immagine.

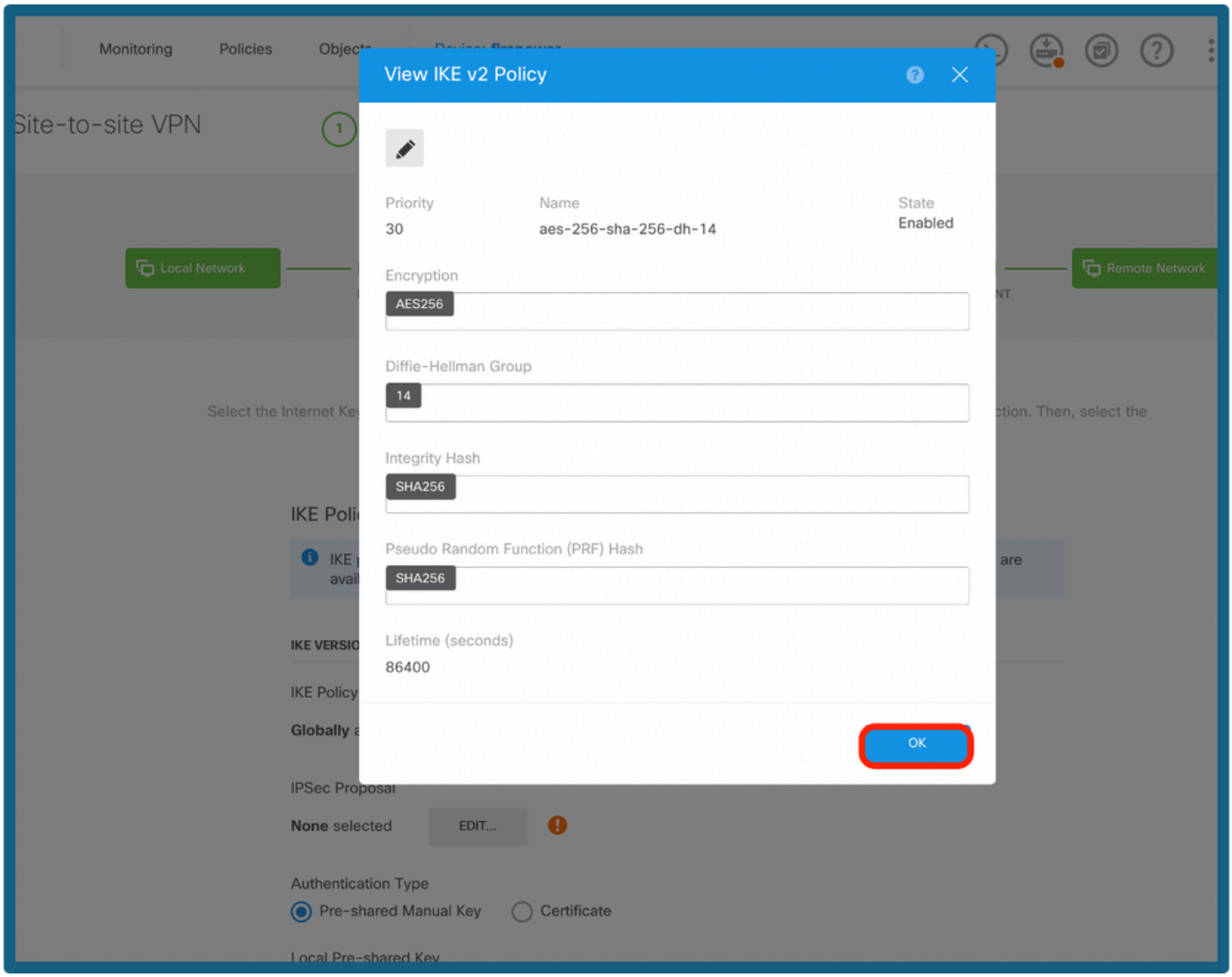


Configura versione IKE

Passaggio 7a. Scegliere il pulsante Criterio IKE come illustrato nell'immagine e fare clic sul pulsante OK o su Crea nuovo criterio IKE per creare un nuovo criterio.

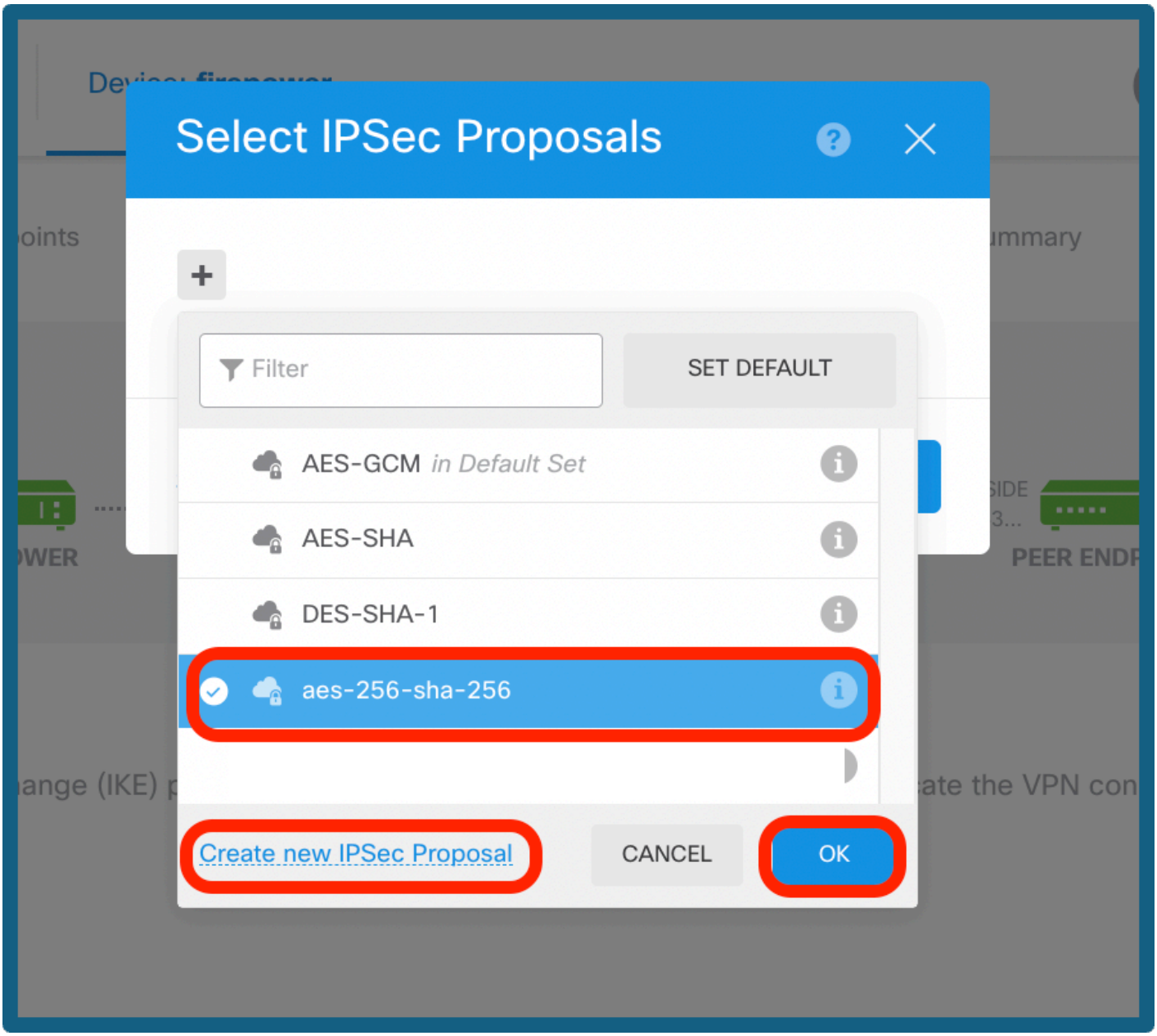


Scegli criterio IKE

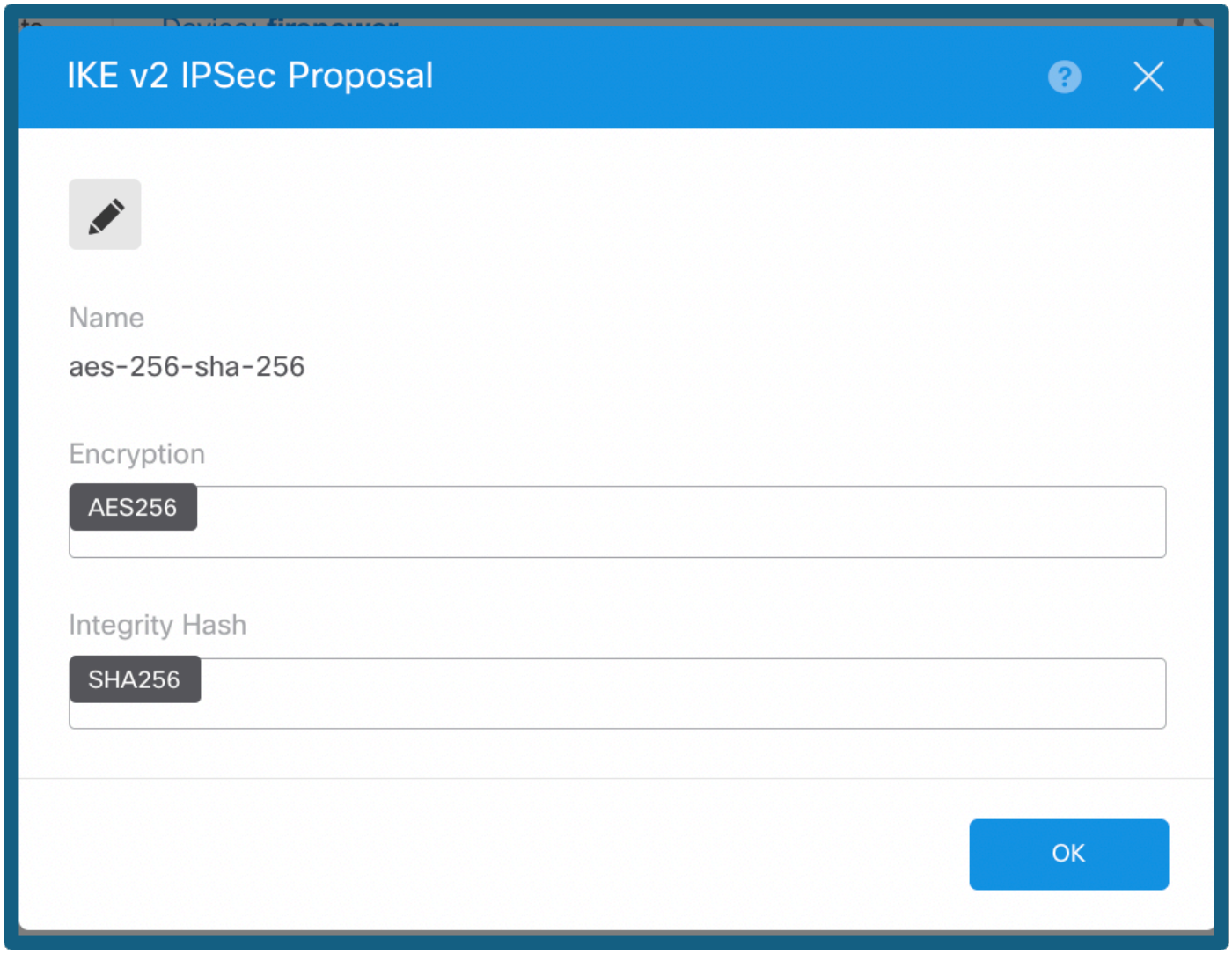


Configurazione del criterio IKE

Passaggio 7b. Scegliere il pulsante Criterio IPSec come illustrato nell'immagine e fare clic sul pulsante OK o su Crea nuova proposta IPSec, se si desidera creare una nuova proposta.



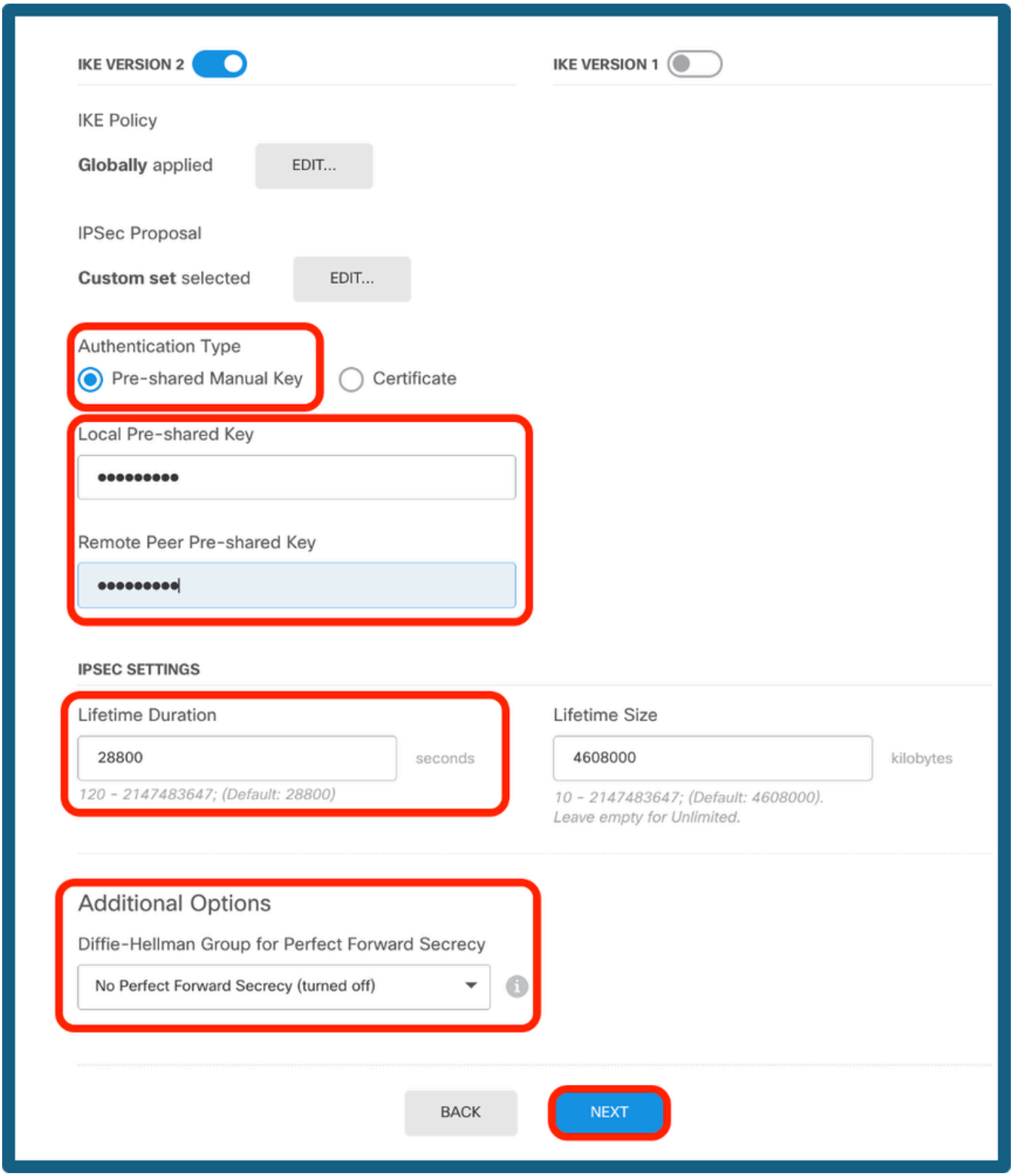
Seleziona proposta IPSec



Configurazione della proposta IPSec

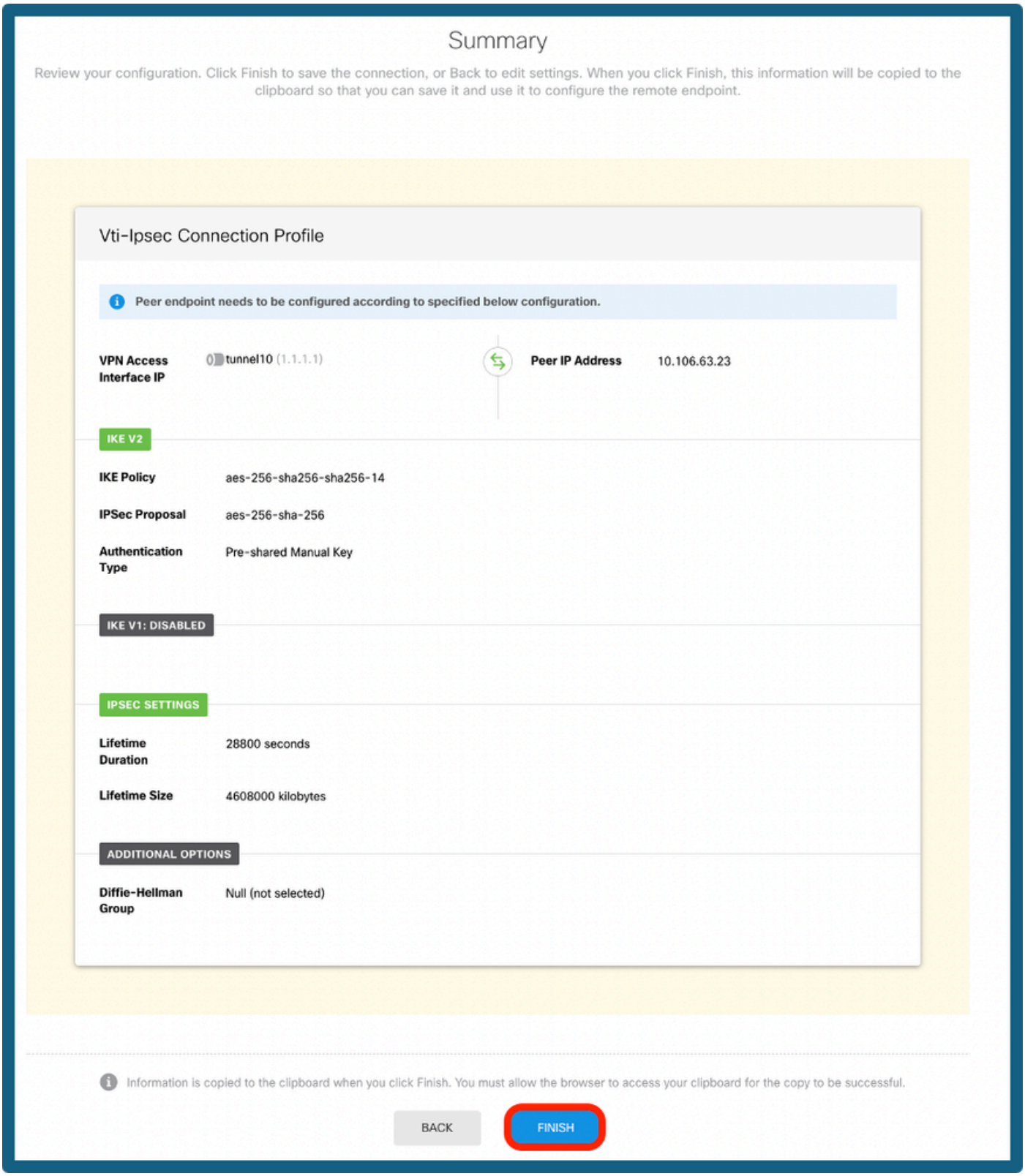
Passaggio 8a. Selezionare il tipo di autenticazione. Se si utilizza una chiave manuale già condivisa, specificare la chiave precondivisa locale e remota.

Passaggio 8b. (Facoltativo) Scegliere le impostazioni Perfect Forward Secrecy. Configurare i campi Durata IPSec e Dimensione durata, quindi fare clic su Avanti.



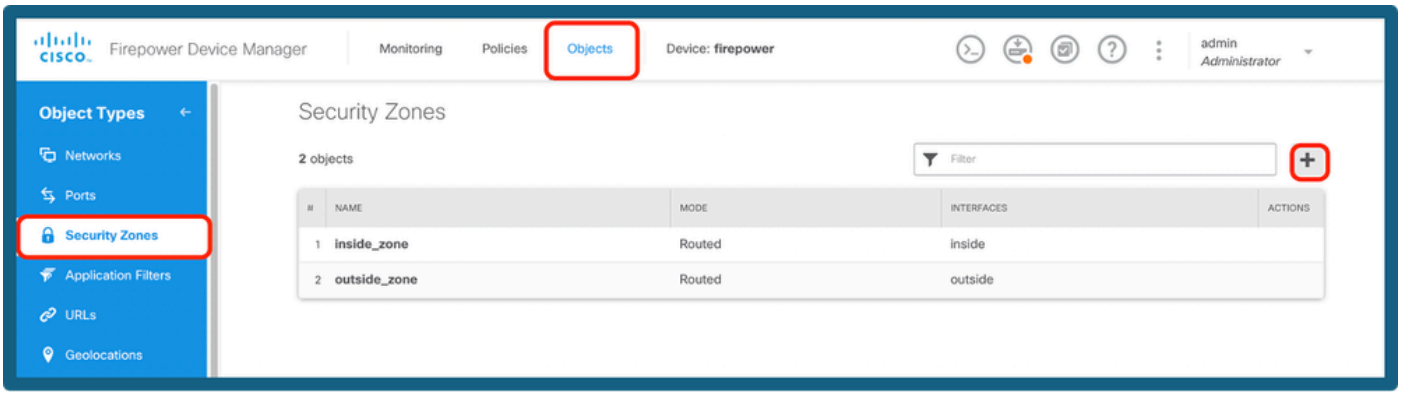
PSK e configurazione durata

Passaggio 9. Esaminare la configurazione e fare clic su Fine.



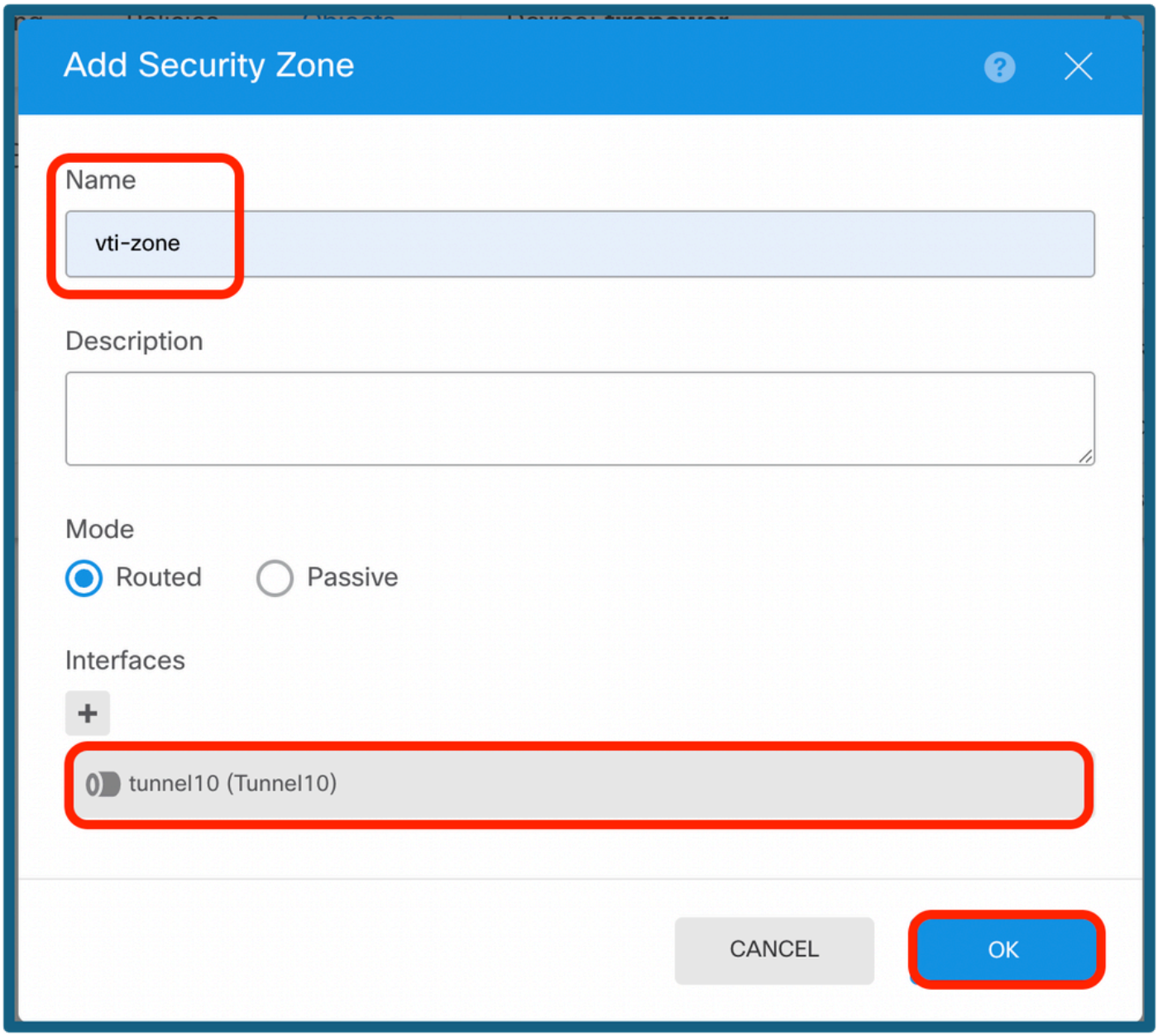
Riepilogo configurazione

Passaggio 10a. Selezionare Oggetti > Aree di sicurezza, quindi fare clic sull'icona +.



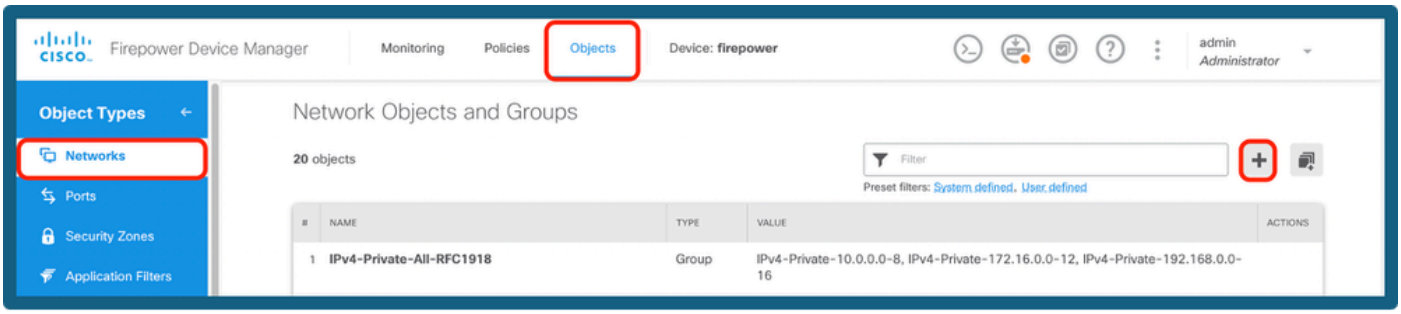
Aggiungi area di sicurezza

Passaggio 10b. Create una zona e selezionate l'interfaccia VTI come mostrato di seguito.



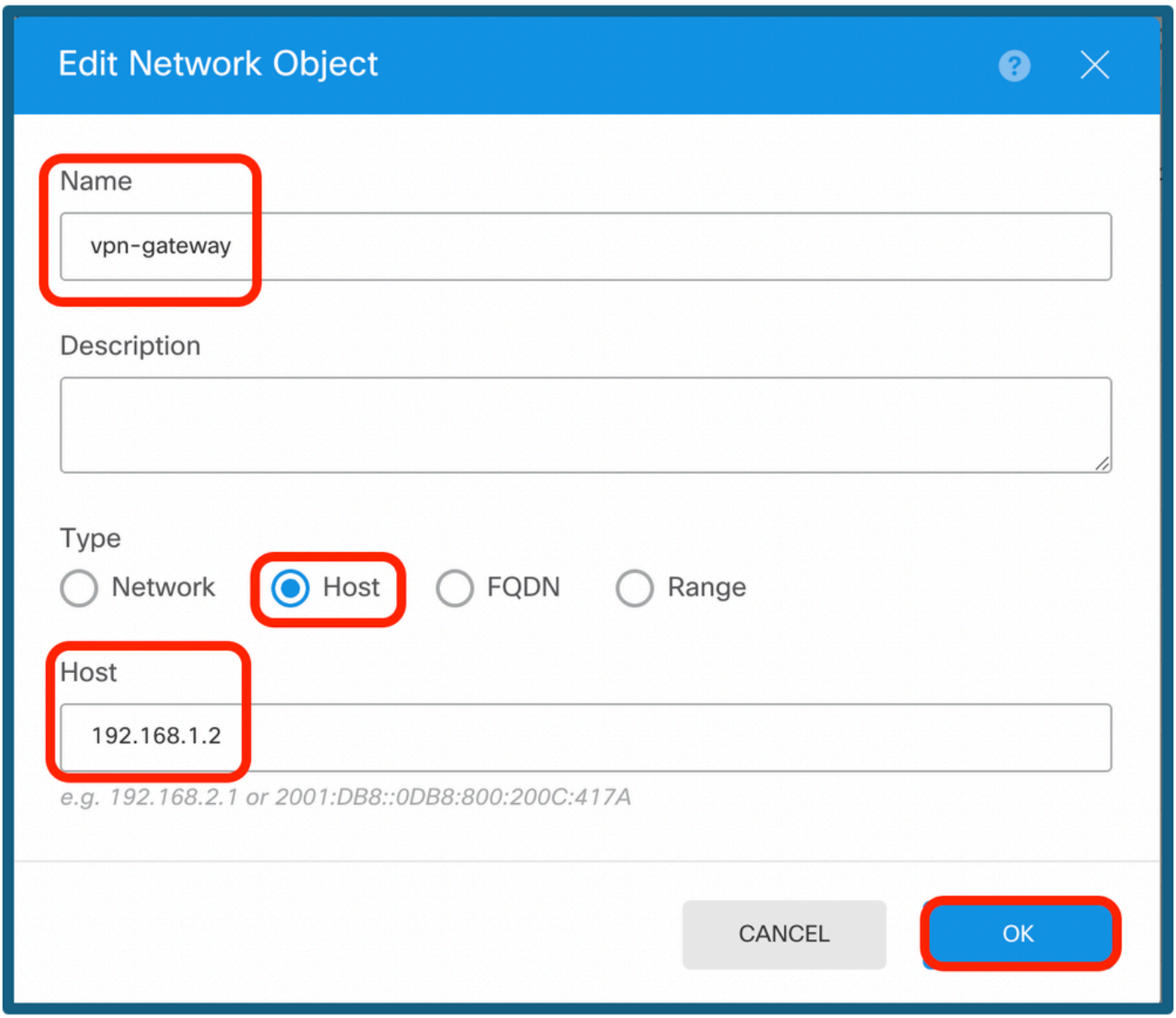
Configurazione dell'area di protezione

Passaggio 11a. Selezionare Oggetti > Reti, quindi fare clic sull'icona +.



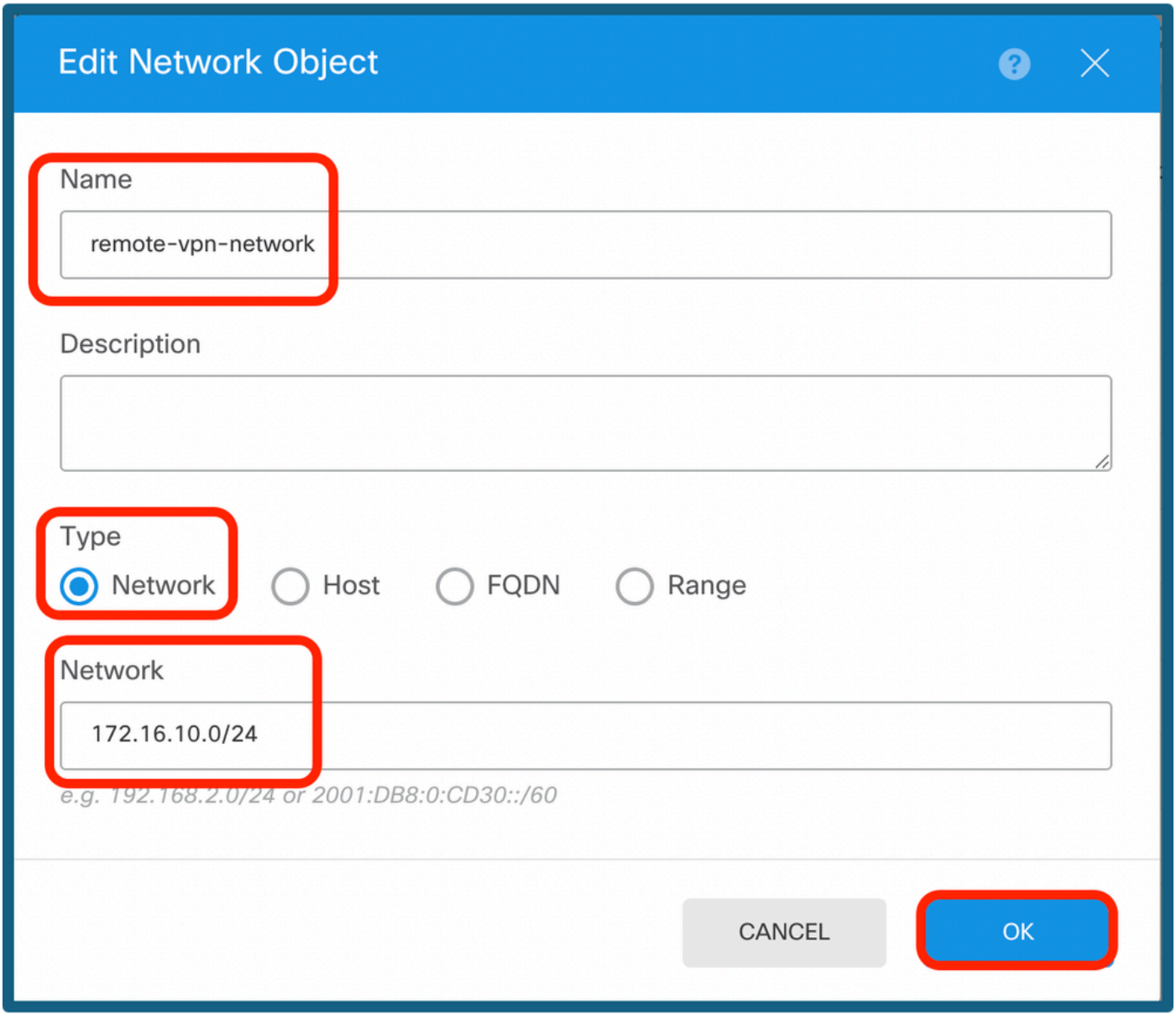
Aggiungi oggetti di rete

Passaggio 11b. Aggiungere un oggetto host e creare un gateway con l'ip del tunnel del peer-end.

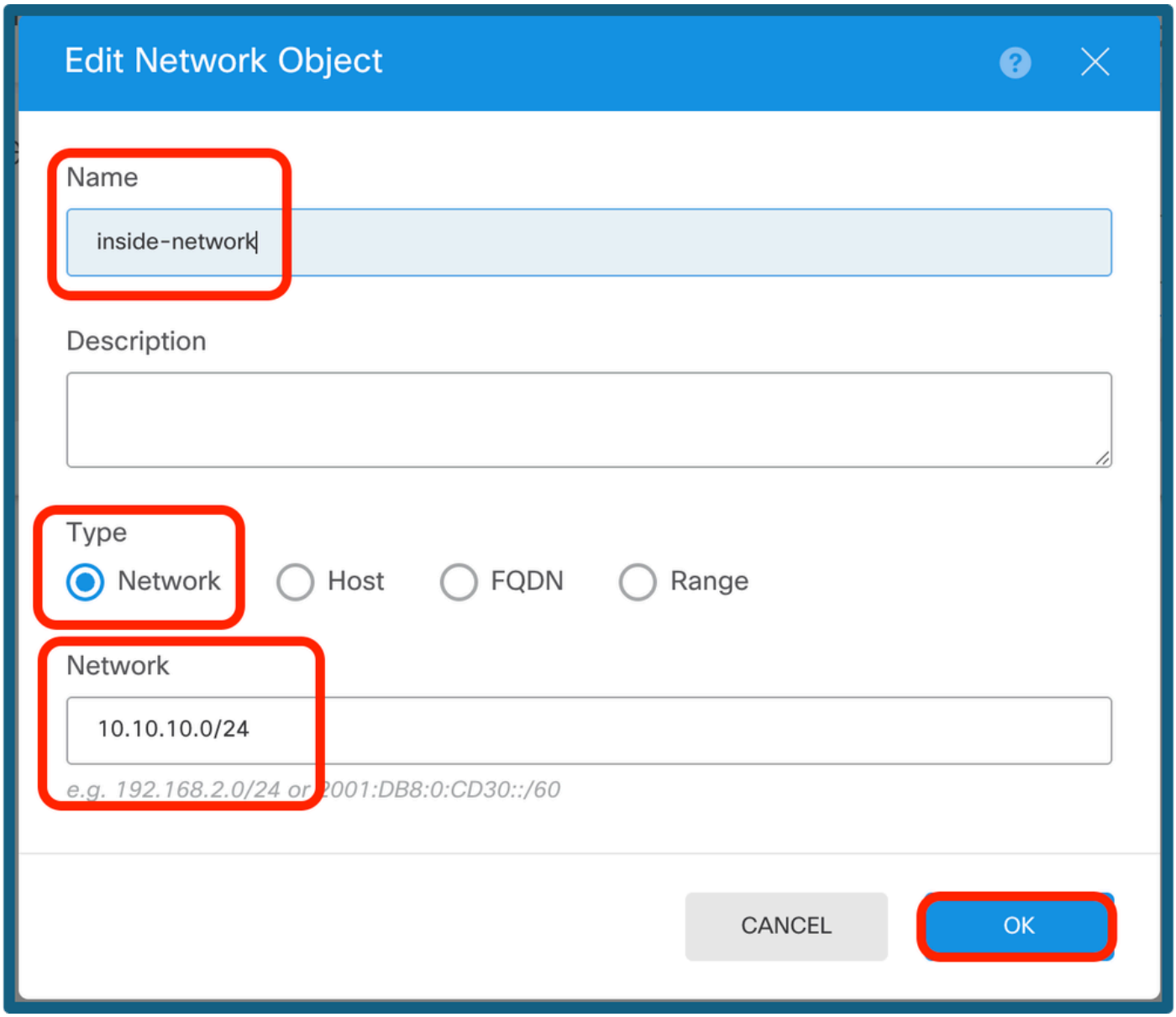


Configura gateway VPN

Passaggio 11c. Aggiungere la subnet remota e la subnet locale.

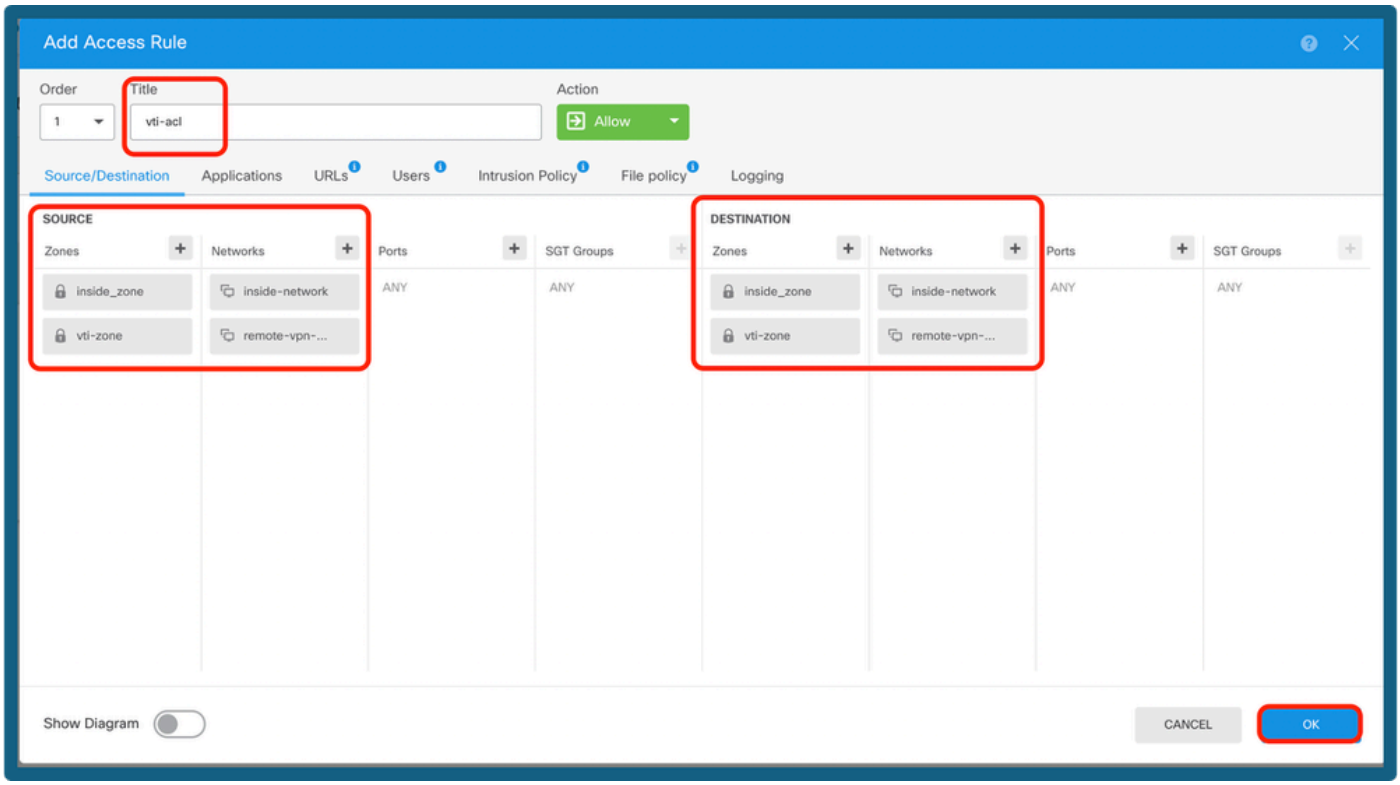


Configurazione IP remoto



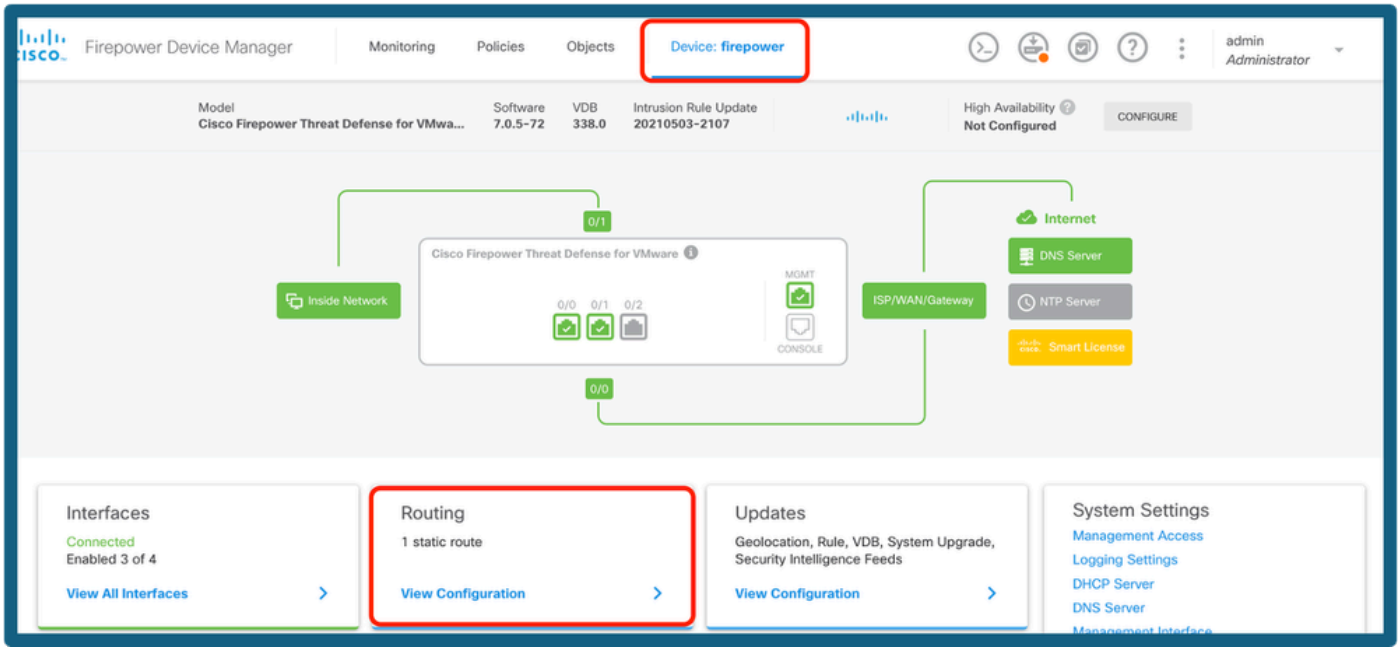
Configurazione IP locale

Passaggio 12. Passare a Periferica > Criteri e configurare i criteri di controllo di accesso.



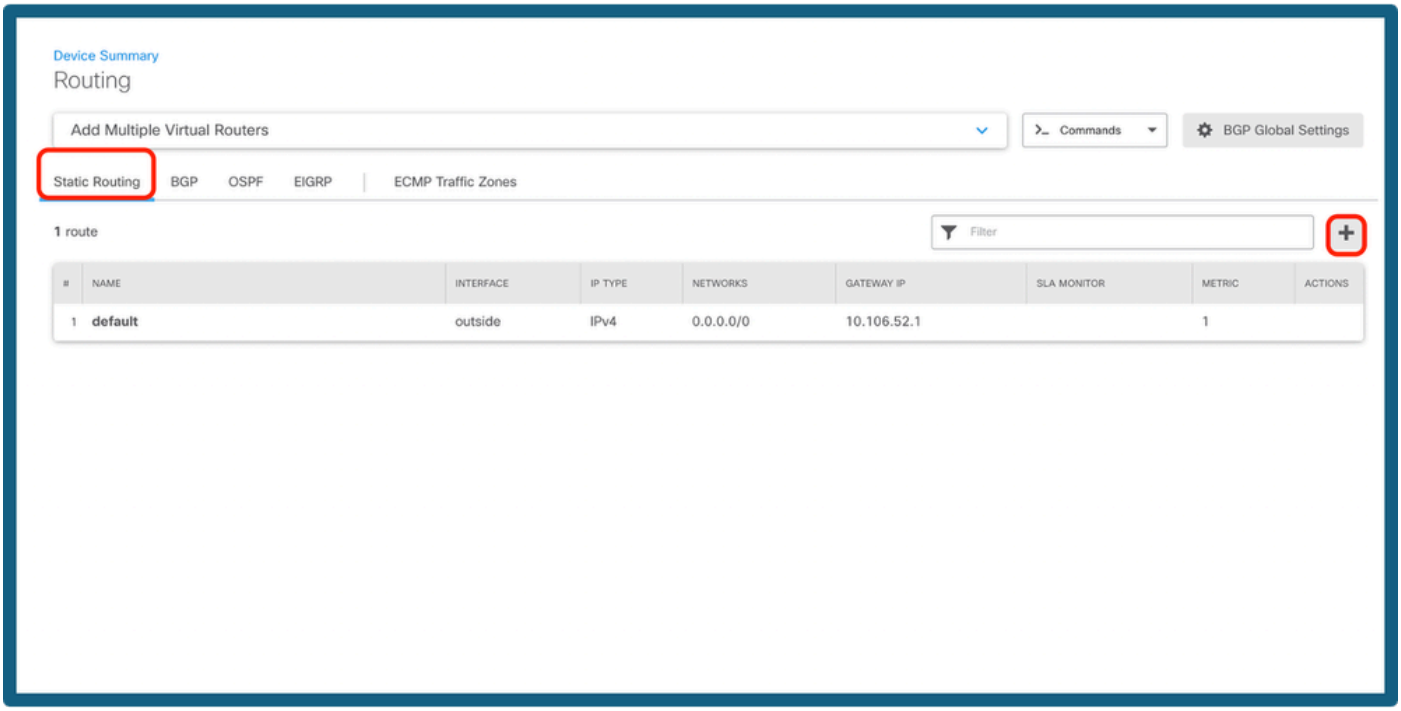
Aggiungi criteri di controllo di accesso

Passaggio 13a. Aggiungere il routing sul tunnel VTI. Selezionare Periferica > Instradamento.



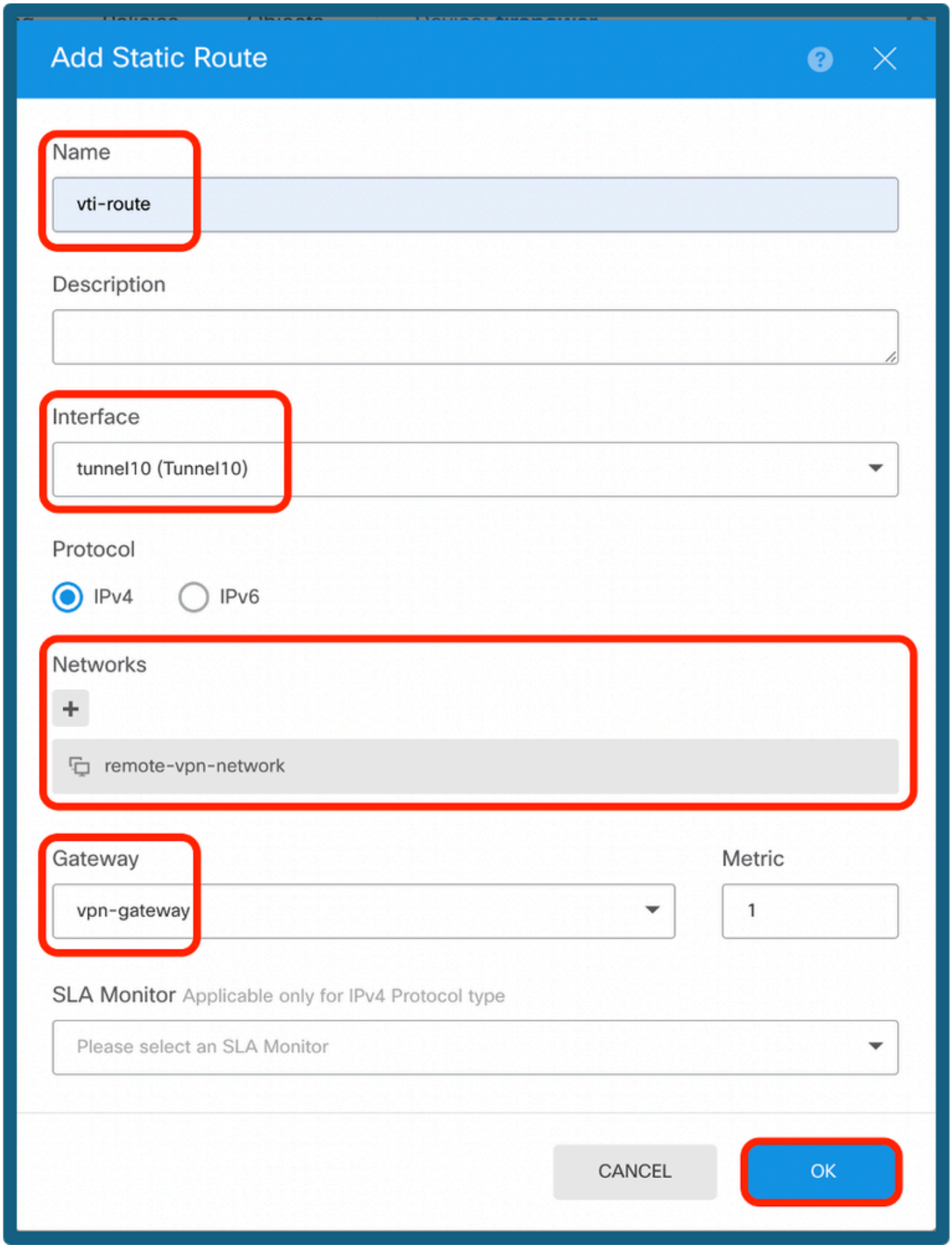
Seleziona ciclo

Passaggio 13b. Passare a Instradamento statico nella scheda Instradamento. Fare clic sull'icona +.



Aggiungi route

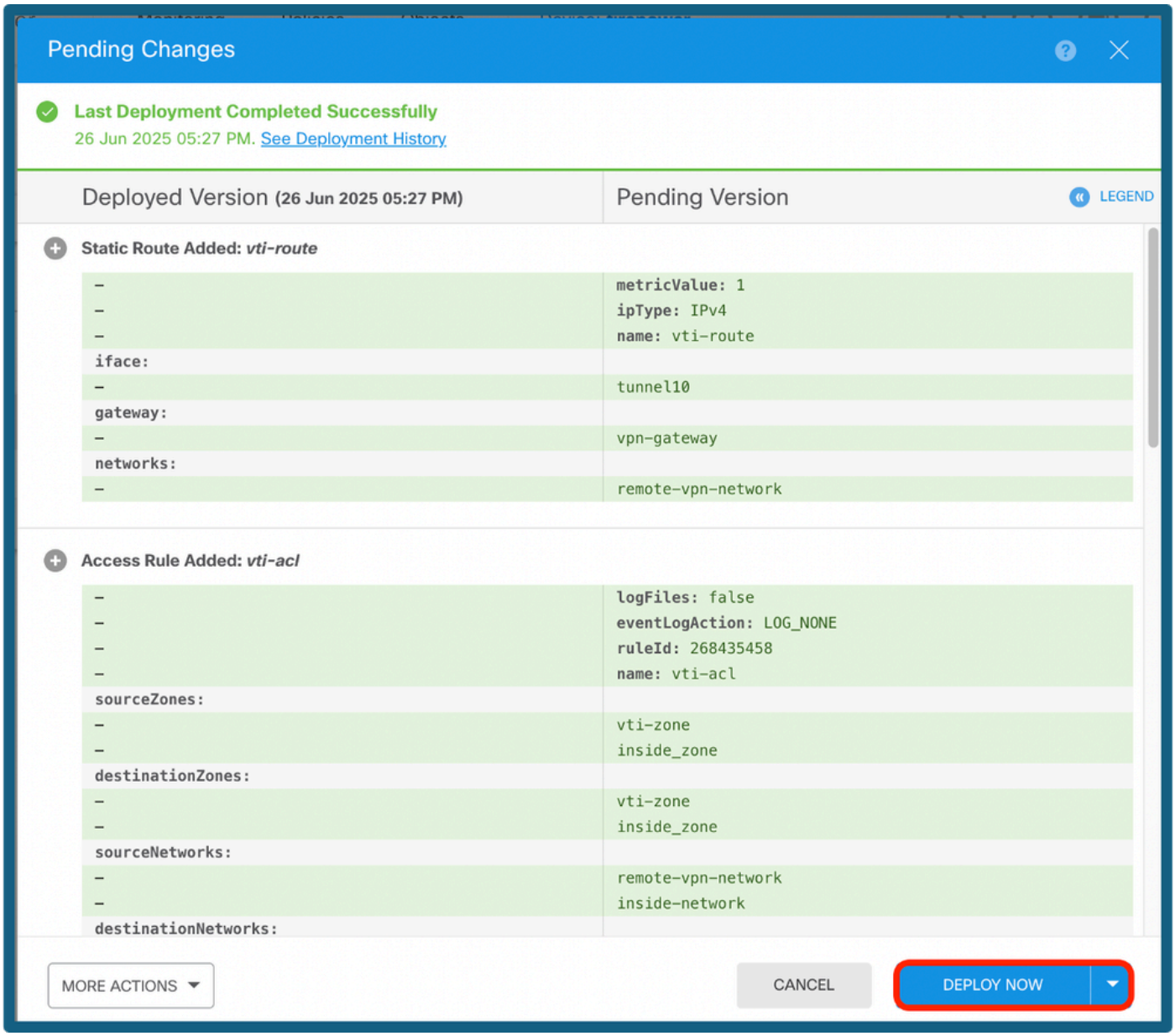
Passaggio 13c. Fornire l'interfaccia, scegliere la rete, fornire il gateway. Fare clic su OK.



Configura route statica

Passaggio 14. Passare a Distribuisci. Rivedere le modifiche, quindi fare clic su Deploy Now

(Distribuisci ora).

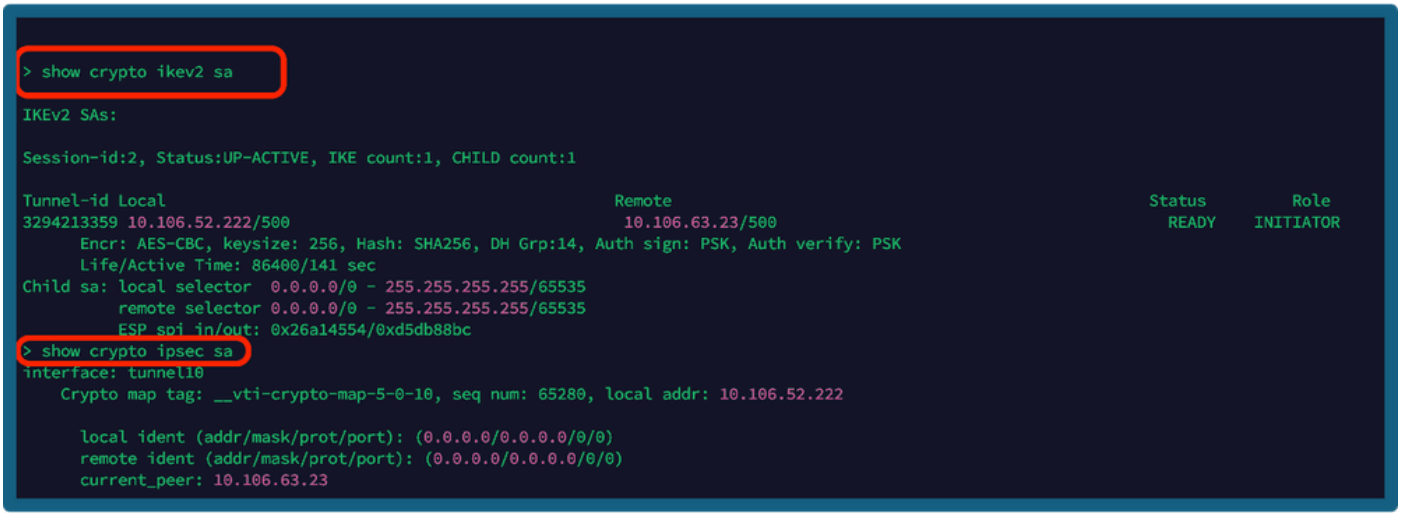


Distribuire la configurazione

Verifica

Una volta completata la distribuzione, è possibile verificare lo stato del tunnel sulla CLI utilizzando i seguenti comandi:

1. show crypto ikev2 sa
2. show crypto ipsec sa <ip-peer>



Comandi show

Informazioni correlate

Per ulteriori informazioni sulle VPN da sito a sito sull'FTD gestito da FDM, è possibile trovare la guida alla configurazione completa qui:

Guida alla configurazione di FTD gestito da FDM

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).